PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-181689
(43)Date of publication of application : 12.07.1996

(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
H04H 1/00
H04N 7/167

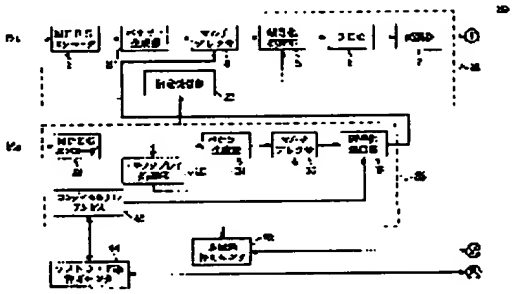
(21)Application number : 07-030056
(22)Date of filing : 25.01.1995

(71)Applicant : SONY CORP
(72)Inventor : KUBOTA YUKIO
GOTO KOICHI

(30)Priority
Priority number : 06289139 Priority date : 28.10.1994 Priority country : JP

(54) DIGITAL SIGNAL TRANSMISSION METHOD, DIGITAL SIGNAL RECEIVER AND RECORDING MEDIUM

(57)Abstract:
PURPOSE: To remarkably improve the security by applying 1st ciphering to a digital signal obtained by applying band compression coding to a video signal, applying ciphering further to the processed signal and sending the resulting signal.
CONSTITUTION: A software supply section 32 uses an MPEG encoder 33 to apply band compression coding to software data PS2 of a digital signal. A trick play section 35 applies processing to extract a picture from video data and provides an output to a multiplexer 36. The digital signal multiplexed by the multiplexer 36 is subject to ciphering of a storage group by a ciphering section 37 and the result is sent to a multiplexer 4 of a transmission section 31. The multiplexer 4 multiplexes the digital signal and a ciphering section 5 applies ciphering of a broadcast group to the multiplexed signal. The digital signal with duplicate security is sent to a digital signal receiver from a satellite.



LEGAL STATUS

[Date of request for examination]	30.03.2000
[Date of sending the examiner's decision of rejection]	25.10.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3729529
[Date of registration]	14.10.2005
[Number of appeal against examiner's decision of rejection]	2002-22757
[Date of requesting appeal against examiner's	25.11.2002

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－181689

(43)公開日　平成８年(1996)７月12日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/00 9/10 9/12			Ｈ０４Ｌ　9/ 00 Ｈ０４Ｎ　7/ 167	Ｚ

審査請求　未請求　請求項の数９　ＦＤ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平7－30056

(22)出願日　平成７年(1995)１月25日

(31)優先権主張番号　特願平6－289139

(32)優先日　平６(1994)10月28日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　久保田　幸雄
東京都品川区北品川６丁目７番35号ソニー株式会社内

(72)発明者　後藤　晃一
東京都品川区北品川６丁目７番35号ソニー株式会社内

(74)代理人　弁理士　田辺　恵基

(54)【発明の名称】　デイジタル信号伝送方法、デイジタル信号受信装置及び記録媒体

(57)【要約】

【目的】本発明は、デイジタル信号伝送方法、デイジタル信号受信装置及び記録媒体について、有料のソフトウエア情報のセキユリテイを確保する。

【構成】所定のサービスを提供する映像を伝送する場合、映像信号を帯域圧縮符号化したデイジタル信号に第１の暗号化処理をした後、当該デイジタル信号にさらに暗号化処理をして伝送する。これにより映像信号に２重のセキユリテイを付加することかできるので、一段とセキユリテイが確保されたデイジタル信号伝送方法を実現し得る。

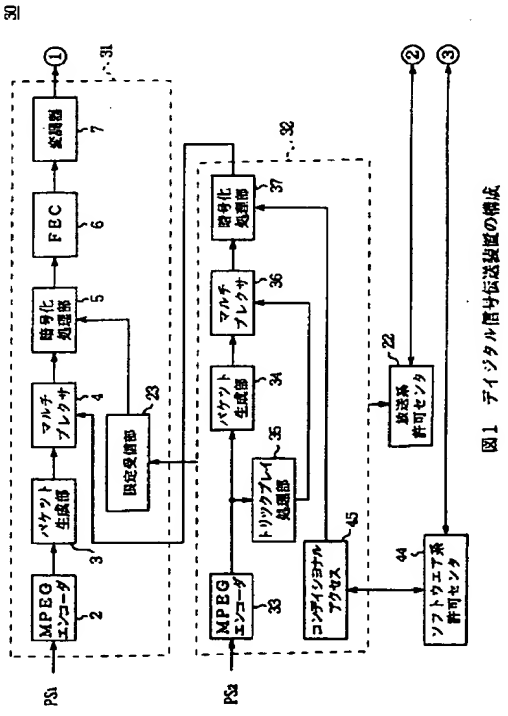


図１　デイジタル信号伝送装置の構成

1

【特許請求の範囲】

【請求項１】少なくとも映像信号を帯域圧縮符号化したデイジタル信号に暗号化処理をして伝送するデイジタル信号伝送方法において、

所定のサービスを提供する映像を伝送する場合には、上記帯域圧縮符号化したデイジタル信号に第１の暗号化処理をした後、当該第１の暗号化処理がなされたデイジタル信号にさらに上記暗号化処理をして伝送することを特徴とするデイジタル信号伝送方法。

【請求項２】上記帯域圧縮符号化されかつ第１の暗号化処理がなされたデイジタル信号と、所定映像単位内で上記帯域圧縮符号化が完結しているデイジタル信号とを混合し、

当該混合信号に上記暗号化処理をして伝送することを特徴とする請求項１に記載のデイジタル信号伝送方法。

【請求項３】上記帯域圧縮符号化したデイジタル信号に上記第１の暗号化処理をする際に用いる第１の暗号化キーを第２の暗号化キーを用いて暗号化することを特徴とする請求項１に記載のデイジタル信号伝送方法。

【請求項４】少なくとも映像信号を帯域圧縮符号化したデイジタル信号に暗号化処理をして伝送するデイジタル信号伝送方法において、

上記帯域圧縮符号化されかつ暗号化処理がなされたデイジタル信号と、所定映像単位内で上記帯域圧縮符号化が完結しているデイジタル信号とを混合して伝送することを特徴とするデイジタル信号伝送方法。

【請求項５】少なくとも映像信号を帯域圧縮符号化したデイジタル信号に第１の暗号をかけた後、第２の暗号をかけて放送局より伝送されるデイジタル信号を受信するデイジタル信号受信装置において、

上記デイジタル信号にかけられた上記第２の暗号を解除する第２の暗号解除手段と、

当該第２の暗号が解除されたデイジタル信号を記録媒体に記録すると共に、当該記録媒体に記録されたデイジタル信号を再生する記録再生手段と、

上記記録媒体より再生される再生信号の上記第１の暗号を解除する第１の暗号解除手段とを具えることを特徴とするデイジタル信号受信装置。

【請求項６】上記第１の暗号解除手段は、上記帯域圧縮符号化したデイジタル信号に上記第１の暗号をかける際に用いる暗号化キーにかけられている暗号を解除する暗号化キー用の暗号解除手段を具え、当該暗号化キー用の暗号解除手段によつて上記暗号化キーにかけられている暗号を解除し、当該暗号が解除された暗号化キーを用いて上記再生信号の第１の暗号を解除することを特徴とする請求項５に記載のデイジタル信号受信装置。

【請求項７】上記放送局は、帯域圧縮符号化したデイジタル信号に第１の暗号をかけたデイジタル信号と所定映像単位内で上記帯域圧縮符号化が完結しているデイジタル信号とを混合して当該混合信号に第２の暗号をかけて伝送し、

2

上記記録再生手段は、上記第１の暗号がかけられたデイジタル信号と所定映像単位内で上記帯域圧縮符号化が完結しているデイジタル信号とを記録し、変速再生時には、上記所定映像単位内で上記帯域圧縮符号化が完結しているデイジタル信号を用いて変速再生画を出力することを特徴とする請求項５に記載のデイジタル信号受信装置。

【請求項８】モデムを有し、課金情報を管理する複数の管理局へのアクセスの切換えを上記モデムを介して制御することにより、上記複数の課金体系を構築することを特徴とするデイジタル信号受信装置。

【請求項９】少なくとも映像信号を帯域圧縮符号化したデイジタル信号に暗号化処理をしたデイジタル信号が記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【目次】以下の順序で本発明を説明する。

【０００２】

【産業上の利用分野】本発明はデイジタル信号伝送方法、デイジタル信号受信装置及び記録媒体に関し、例えば有料のソフトウエア情報を契約ユーザに提供するデイジタル信号伝送システムに適用して好適なものである。

【０００３】

【従来の技術】従来、衛星又はケーブルによるデイジタル信号伝送システムにおいては、図９に示すように、デイジタル信号伝送装置すなわち放送局１において、入力されるプログラムソースＰＳをＭＰＥＧ（Moving Picture Image Coding Experts Group）エンコーダ２でＭＰＥＧ方式で帯域圧縮符号化してパケツト生成部３でパケツト化する。

【０００４】パケツト化された伝送データはマルチプレクサ４で多重化された後、暗号化処理部５で伝送データ

にセキュリテイとしてスクランブルをかけ、さらにこのスクランブルが簡単に解けないように何重にも鍵（暗号）をかける。暗号化された伝送データはＦＥＣ(forward error correction)部６でエラー訂正されて変調器７で変調された後、デイジタル衛星８を介して契約ユーザの家庭内に設置されているデイジタル信号受信装置すなわち端末１０（図１０）に直接送出されるか、又は衛星８を介してヘツドエンドと呼ばれる配信局９（図１０）に送出され、配信局９よりケーブルを介して端末１０に送出される。

【０００５】ここで図１０に示すように、端末１０では、伝送データが衛星８を介して直接送られてきた場合には伝送データはアンテナ１１で受信されてフロントエンド部１２に送出され、伝送データが配信局９よりケーブルを介して送られてきた場合にはフロントエンドブロツク１２に直接入力される。放送局１と契約したユーザは、衛星８より直接又は衛星８より配信局９を介して送られてきた伝送データに対し、ユーザ毎に許可されたキーを端末１０にアクセスすることにより、契約ユーザとしてオーソライズ（許可）されて課金処理されると同時に所望のソフトウエア情報を鑑賞することができる。

【０００６】すなわち端末１０において、チユーナ、復調器及びエラー訂正器で構成されるフロントエンド部１２で処理された伝送データはデータ取出し部１３に入力される。データ取出し部１３では、まずデマルチプレクサ１４で多重化を解除して、映像信号、音声信号及びこれ以外のデータに分離する。暗号解除部１５では、課金処理と同時に暗号を解除し、パケツト分離部１６でパケツト分離した後、ＭＰＥＧデコーダ１７で圧縮を解凍（伸長）すると共にデイジタル／アナログ変換して映像信号及び音声信号をテレビジヨン（ＴＶ）に出力する。

【０００７】

【発明が解決しようとする課題】ところでデイジタル信号伝送システムでは、ビデオオンデマンド(video on demand）やニアビデオオンデマンド(near video on demand)などの有料のソフトウエア情報を伝送する場合、ユーザの便宜を図ると共にデイジタル伝送路を有効に活用する手段として、端末１０にテープメデイアやデイスクメデイアのデイジタルストレージ１８を内蔵又は接続している。この場合、空き時間帯又は空き伝送路を利用して大容量のソフトウエアデータをストレージ１８にダウンロードしておき、ユーザが手元のソフトウエア情報を観るときには、ＩＤカード（例えばスマートカード）１９でアクセスすることによつて課金処理が行われて再生制限が解かれる。

【０００８】すなわちユーザがスマートカード１９でアクセスすると、中央処理装置（ＣＰＵ）２０がモデム２１を介して許可センタ２２（図９）に登録の問い合わせを行う。許可センタ２２は、コンデイシヨナルアクセス(Conditional Access) ２３によつて登録を確認し、登録が確認されると、許可センタ２２は課金処理をすると共にモデム２１を介してＣＰＵ２０に確認の通知を行う。

【０００９】ＣＰＵ２０はこの通知によつてローカルコンデイシヨナルアクセス (Local Conditional Access) ２４にキーの解除を指示し、ローカルコンデイシヨナルアクセス２４はストレージ１８に記録されているデータにかけられている暗号を解除する。これにより再生制限が解かれ、ストレージ１８に記録されているデータはパケツト分離部１６でパケツトが分離される。パケツト分離されたデータはＭＰＥＧデコーダ１７で圧縮が解凍された後、デイジタル／アナログ変換されて音声信号及び映像信号Ａ／ＶとしてＴＶに出力される。

【００１０】ところが現行の放送形態におけるセキュリテイシステムで、上述のようにストレージ１８にソフトウエア情報をダウンロードしておき、観たいときにこのソフトウエア情報を鑑賞し得るようなシステムを実現しようとすると、以下のような問題点が生ずる。

【００１１】すなわち現行のデイジタル信号伝送システムでは、図１１に示すように、暗号解除部１５で暗号を解除した後にストレージ１８にソフトウエア情報をダウンロードする場合（図１１のＡ点）、暗号を解除することはすなわち課金することであるので、有料ソフトを課金なしに暗号を解除してストレージ１８にダウンロードすることはできない。ここで課金情報だけを無料として全てのデータの暗号を解除してストレージ１８にダウンロードすると、１つのソフトウエア情報についてはそのままスルーで端末１０より出力されてしまう。

【００１２】またストレージ１８が端末１０に内蔵されておらず端末１０に接続され、暗号解除部１５とパケツト分離部１６との間にスイツチング手段が設けられていない場合には、暗号を全て解除してストレージ１８にダウンロードすると、暗号が解除されたデータが全て送出され、図１１のＣ点において契約者以外の者にただで観られるおそれがあつた。

【００１３】このような問題点を解決するために、暗号を解除する前、すなわちデマルチプレクサ１４で多重化が解除された後（図１１のＢ点）、ストレージ１８にダウンロードすることが考えられる。ところがデマルチプレクサ１４で多重化が解除された後ストレージ１８にダウンロードすると、暗号化されたままの状態であるのでＩ（intra-coded ）ピクチヤを抜き出すことができず、変速再生することができないという問題があつた。

【００１４】また放送系でデータを暗号化するシステムでは、セキュリテイを確保するために１年とか２年毎にキーを変えるため、ストレージ１８にソフトウエア情報をダウンロードした後にキーの変更があつた場合、暗号を解除することができずダウンロードしたソフトウエア情報を観ることができないという問題があつた。

【００１５】本発明は以上の点を考慮してなされたもの

で、有料のソフトウエア情報を伝送する場合のセキュリティを確保し得るデイジタル信号伝送方法、デイジタル信号受信装置及び記録媒体を提案しようとするものである。

【００１６】

【課題を解決するための手段】かかる課題を解決するため本発明においては、少なくとも映像信号を帯域圧縮符号化したデイジタル信号に暗号化処理をして伝送するデイジタル信号伝送方法において、所定のサービスを提供する映像を伝送する場合には、帯域圧縮符号化したデイジタル信号に第１の暗号化処理をした後、当該第１の暗号化処理がなされたデイジタル信号にさらに暗号化処理をして伝送する。

【００１７】また本発明においては、少なくとも映像信号を帯域圧縮符号化したデイジタル信号に暗号化処理をして伝送するデイジタル信号伝送方法において、帯域圧縮符号化されかつ暗号化処理されたデイジタル信号と、所定映像単位内で帯域圧縮符号化が完結しているデイジタル信号とを混合して伝送する。

【００１８】また本発明においては、少なくとも映像信号を帯域圧縮符号化したデイジタル信号に第１の暗号をかけた後、第２の暗号をかけて放送局より伝送されるデイジタル信号を受信するデイジタル信号受信装置（４０）において、デイジタル信号にかけられた第２の暗号を解除する第２の暗号解除手段（（１５）、（１９））と、当該第２の暗号が解除されたデイジタル信号を記録媒体に記録すると共に、当該記録媒体に記録されたデイジタル信号を再生する記録再生手段（（７３）、（７４）、（７５）、（７６）、（７７））と、記録媒体より再生される再生信号の第１の暗号を解除する第１の暗号解除手段（（４６）、（９１））とを設ける。

【００１９】また本発明においては、少なくとも映像信号を帯域圧縮符号化したデイジタル信号に暗号化処理をした信号が記録されている記録媒体（１０１）を設ける。

【００２０】

【作用】所定のサービスを提供する映像を伝送する場合、映像信号を帯域圧縮符号化したデイジタル信号に第１の暗号化処理をした後、当該デイジタル信号にさらに暗号化処理をして伝送する。これにより、映像信号に２重のセキュリティを付加することかできるので、一段とセキュリティが確保されたデイジタル信号伝送方法を実現し得る。

【００２１】また少なくとも映像信号を帯域圧縮符号化しかつ暗号化処理したデイジタル信号と、所定映像単位内で帯域圧縮符号化が完結しているデイジタル信号とを放送局（３０）で混合する。これにより、端末（４０）で変速再生処理をせずに変速再生画を観ることができる。

【００２２】少なくとも映像信号を帯域圧縮符号化したデイジタル信号に第１の暗号及び第２の暗号をかけて放送局（３０）より伝送されるデイジタル信号を受信すると、受信したデイジタル信号にかけられた第２の暗号を第２の暗号解除手段（（１５）、（１９））で解除した後、当該第２の暗号が解除されたデイジタル信号を記録再生手段（（７３）、（７４）、（７５）、（７７））によつて記録媒体に記録する。再生時には、記録媒体より再生される再生信号の第１の暗号を第１の暗号解除手段（（４６）、（９１））で解除する。これにより、セキュリテイが一段と確保されたデイジタル信号受信装置（４０）を実現し得る。

【００２３】また少なくとも映像信号を帯域圧縮符号化したデイジタル信号に暗号化処理をした信号が記録されている記録媒体（１０１）を用意する。これにより、契約ユーザは暗号がかけられたソフトウエア情報が記録された記録媒体（１０１）をローコストで入手することができ、観たい部分だけを課金処理して楽しむ新しいソフトウエア供給システムを構築することができる。

【００２４】

【実施例】以下図面について、本発明の一実施例を詳述する。

【００２５】（１）デイジタル信号伝送装置及びデイジタル信号受信装置の構成

図９との対応部分に同一符号を付して示す図１において、３０は全体として本発明の実施例によるデイジタル信号伝送装置を示している。デイジタル信号伝送装置３０すなわち放送局においては、所定のサービス例えば有料のソフトウエア情報を伝送する場合、予めソフトウエアデータにストレージ系の暗号をかけた後、当該ソフトウエアデータにさらに放送系の暗号をかけて２重のセキュリテイを確保している。

【００２６】デイジタル信号伝送装置３０はデイジタル信号送出部３１及びソフトウエア供給部３２によつて構成されている。デイジタル信号伝送装置３０において、ユーザより有料のソフトウエア情報、例えば映像ソフト、音楽ソフト、電子番組表、シヨツピング情報、ゲームソフトや教育情報などが要求された場合には、図１に示すように、プログラムソースPS_2としてのこれらのソフトウエア情報がソフトウエア供給部３２に入力される。

【００２７】ソフトウエア供給部３２では、まずデイジタル信号でなるソフトウエアデータPS_2をＭＰＥＧエンコーダ３３で帯域圧縮符号化する。帯域圧縮符号化されたデイジタル信号はパケツト生成部３４及びトリツクプレイ処理部３５に入力される。トリツクプレイ処理部３５では映像データについて変速再生処理すなわちＩ(intra-coded) ピクチヤを抜き出す処理をして、抜出したＩピクチヤをマルチプレクサ３６に出力する。ここでＭＰＥＧ方式で帯域圧縮符号化された映像を変速再生し得るようにするための技術については、特願平5-287702号

に記載されている。

【００２８】パケット生成部３４では、入力されたデイジタル信号を映像データ、音声データ及びこれ以外のデータ毎にパケット化してマルチプレクサ３６で多重化する。このマルチプレクサ３６で映像データにＩピクチャが埋め込まれる。多重化されたデイジタル信号は暗号化処理部３７でストレージ系の暗号をかけた後送出部３１のマルチプレクサ４に送出される。

【００２９】マルチプレクサ４では、ストレージ系の暗号がかけられたデイジタル信号を多重化し、暗号化処理部５でこの多重化されたデイジタル信号に放送系の暗号をかける。従つてデイジタル信号伝送装置３０より送出されるデイジタル信号には、ストレージ系の暗号と放送系の暗号が２重にかけられている。ここで送出部３１で各プログラムに付加されるキーデータは全て共通であり、放送による課金データは無料である。

【００３０】この２重のセキュリテイが付加されたデイジタル信号は、図１０との対応部分に同一符号を付して示す図２に示すように、衛星８より直接又は衛星８より配信局９を介して家庭内に設置された端末、すなわちデイジタル信号受信装置４０に送られる。デイジタル信号受信装置４０では、スマートカード１９をアクセスすることによつて、伝送されるデイジタル信号にかけられた放送系の暗号を解除し、当該デイジタル信号をデイジタルストレージ４１にダウンロードすることができる。すわなち伝送されるデイジタル信号は、暗号解除部１５において放送系の暗号が解除された後、デイジタルストレージ４１に記録される。

【００３１】この場合、デイジタルストレージ４１にダウンロードされるデイジタル信号には、ストレージ系の暗号だけがかかつた状態で記録され、しかも変速再生処理がなされた状態で記録される。従つて送出部３１で付加された放送系のキーが変更されても影響はなく、また図２のＣ点においてはストレージ系の暗号がかかつているため映像をただで観られることはない。

【００３２】ストレージ４１にダウンロードされたソフトウエア情報PS_2を観る場合には、放送系とは別に登録されたＩＤ番号を入力する（例えばパーソナルコンピュータの画面上でＩＤ番号を入力する）ことにより、ＣＰＵ４２がモデム４３を介してソフトウエア情報用の許可センタ４４（図１）に登録の問い合わせをする。ここでＣＰＵ４２は通常契約によるプログラムPS_1については放送系の許可センタ２２に登録の問い合わせをし、ソフトウエア情報PS_2についてはソフトウエア系の許可センタ４４に登録の問い合わせをする。すなわちＣＰＵ４２はモデム４３のシエアを制御することにより、放送系とソフトウエア系の２つの独立した課金体系を構築している。

【００３３】許可センタ４４はＩＤ番号をソフトウエア供給部３２のコンデイショナルアクセス４５（図１）に送つて登録を確認する。許可センタ４４が登録を確認すると課金処理がなされ、ＣＰＵ４２はローカルコンデイショナルアクセス４６に暗号の解除を指示する。ここでローカルコンデイショナルアクセス４６はソフトウエア系の暗号を解除する機能を有する。これによりストレージ４１の再生制限が解除されて暗号が解除され、ユーザは解除された部分だけ通常のＶＴＲ（video tape recorder）と同じ操作でソフトウエア情報を観ることができる。

【００３４】（２）実施例によるデイジタル信号伝送装置の構成

実施例によるデイジタル信号伝送装置の送出部３１及びソフトウエア供給部３２の詳細構成をそれぞれ図３及び図４に示す。このデイジタル信号伝送装置３０において、通常契約のプログラムPS_1を供給する場合には、プログラムソースPS_1は送出部３１に直接入力され、有料のソフトウエア情報を供給する場合には、当該ソフトウエア情報PS_2はソフトウエア供給部３２を介して送出部３１に供給される。

【００３５】プログラムPS_1の鑑賞については、例えば業務用デイジタルＶＴＲ４７より供給されるプログラムの映像信号及び音声信号はそれぞれＭＰＥＧエンコーダ２Ａ、２Ｂで帯域圧縮符号化された後、パケット生成部３Ａ、３Ｂで画像及び音声毎にパケット化されてデータバス４８を介してマルチプレクサ４に送出される。これと同時に、例えばパーソナルコンピユータ（以下パソコンと呼ぶ）４９によつて映像データ及び音声データ以外のデータがデータインタフエース（データＩ／Ｆ）５０を介してパケット生成部３Ｃに送出されてパケット化された後、データバス４８を介してマルチプレクサ４に送出される。

【００３６】またコンデイショナルアクセス２３よりキーデータがデータＩ／Ｆ５１を介してパケット生成部３Ｄに送出されてパケット化され、データバス４８を介してマルチプレクサ４に送出される。さらにコンデイショナルアクセス２３はソフトウエアデータを暗号化するためのキー情報を暗号化処理部５に送出する。マルチプレクサ４では、映像、音声及びこれ以外のデータを多重化し、暗号化処理部５において、コンデイショナルアクセス２３より入力されたキー情報に基づいてこの多重化されたデータに暗号をかける。暗号化されたデータはＦＥＣ部６でエラー訂正されて変調器７で変調された後、アツプコンバータ５２を介して衛星８に伝送される。

【００３７】これに対して有料のソフトウエア情報PS_2を伝送する場合には、図４に示すように、例えばデイジタルＶＴＲ５３より出力されるソフトウエア情報PS_2の映像信号及び音声信号はそれぞれＭＰＥＧエンコーダ３３Ａ、３３Ｂで帯域圧縮符号化される。帯域圧縮符号化された映像信号はパケット生成部３４Ａ及びトリツクプレイ処理部３５に入力される。パケット生成部３４

Ａでは入力された映像信号をパケツト化し、トリツクプレイ処理部３５では入力される映像信号より１ピクチヤを抜き出して、このＩピクチヤをマルチプレクサ３６に出力する。

【００３８】帯域圧縮符号化された音声信号はパケツト生成部３４Ｂでパケツト化される。またパソコン５４より入力される映像及び音声以外の一般データがデータＩ／Ｆ５５を介してパケツト生成部３４Ｃに送出される。またコンデイシヨナルアクセス４５はキーデータをデータＩ／Ｆ５６を介してパケツト生成部３４Ｄに送出すると共に、ストレージ系のキー情報を暗号化処理部３７に送出する。

【００３９】各パケツト生成部３４でそれぞれパケツト化されたデータは、データバス５７を介してマルチプレクサ３６で多重化されると共に、映像データにＩピクチヤが埋め込まれる。多重化されたデータは、暗号化処理部３７において、コンデイシヨナルアクセス４５より入力されたキー情報に基づいて暗号化された後、送出部３１のデータＩ／Ｆ５８（図３）を介してパケツト生成部３Ｅに入力される。パケツト生成部３Ｅでパケツト化されたデータは、データバス４８を介してマルチプレクサ４で多重化されて暗号化処理部５で放送系の暗号がかけられた後、ＦＥＣ部６、変調器７及びアツプコンバータ５２で各処理がなされて衛星８より直接又は衛星８より配信局９を介して端末４０に伝送される。

【００４０】（３）実施例によるデイジタル信号受信装置の構成

実施例によるデイジタル信号受信装置４０は、図２との対応部分に同一符号が付された図５及び図６に示すように、デイジタル信号伝送装置３０より送出されるデイジタル信号を受信する受信部６０（図５）と、受信部６０で受信した信号を記録媒体に記録し再生する記録再生部６１（図６）とによつて構成されている。この実施例の場合、受信部６０と記録再生部６１とはデイジタルインタフエース（デイジタルＩ／Ｆ）６２、６３を介して接続されている。

【００４１】受信部６０では、衛星８より直接又は衛星８より配信局９を介して伝送されるデイジタル信号は圧縮されたデイジタル信号としてチユーナ１２Ａに入力される。チユーニングされたデイジタル信号は、復調器１２Ｂで復調されてＦＥＣ部１２Ｃでエラー訂正された後、デマルチプレクサ１４及び暗号解除部１５でなる暗号解除ブロツクに入力される。暗号解除ブロツクでは、登録されたユーザだけがもつことのできるキーによつて放送系の暗号が解除される。

【００４２】放送系の暗号が解除された一般データ及び所定バイト長のパケツトを単位として複数のプログラムチヤンネルが時分割多重された画像データは、パケツト分離部１６又は記録再生部６１に送出される。パケツト分離部１６に送出される経路と記録再生部６１に送出される経路との切換えはスイツチング手段（図示せず）によつて行われ、この実施例では、スイツチング手段が記録再生部６１に切り換えられているものとする。ここで一般データには、例えばＴＶモニタ上でユーザインタフエースを司るためのテキストデータ、フオントデータ、イメージデータ、グラフイツクデータや動画像データなどが含まれる。

【００４３】一般データはインタラクテイブな処理を行うＣＰＵブロツク６４にデータポートを介して入力される。ＣＰＵブロツク６４は、メインＣＰＵ４２、ＥＥＰＲＯＭ（electrically erasable programmable read only memory）６５、モデムインタフエース（モデムＩ／Ｆ）６６、モデム４３、ＶＲＡＭ（video random access memory）６７、ＧＰＵ（graphic processor unit）６８、ＲＯＭ（read only memory）６９及びＤＲＡＭ（dynamic random access memory）７０によつて構成されている。ここでハードデイスクを内蔵するシステムの場合には、一般データはＣＰＵバスを介して一度ハードデイスク内に格納される。これらの一般データはユーザが外部よりコントローラによつて操作された指示に従つてＣＰＵ４２で処理がなされ、必要な表示データが出力される。

【００４４】一方画像データは、図６に示すようにデイジタルＩ／Ｆ６２、６３を介して記録再生部６１に入力された後、パケツト分離部７１でパケツト分離される。パケツト分離されたデータは、ＴＢＣ(time base corrector) 処理されて、フオーマツト変換部７２でフオーマツトが変換される。フオーマツト変換されたデータはエラー訂正されてローカルコンデイシヨナルアクセス４６を介して変調された後、記録／再生処理部７３によつてメカデツキ７４内の記録媒体に記録される。ここで記録媒体としては、テープ及びデイスクの双方が考えられ、例えばデイジタルＶＣＲ、デイジタルビデオデイスク（ＤＶＤ）、ハードデイスクやミニデイスクなどがある。

【００４５】ユーザより再生の指示があつた場合には、ＣＰＵ４２からＶＣＲコントローラ７５にデイジタルＩ／Ｆ６２、６３を介してコマンドが入力される。ＶＣＲコントローラ７５はこのコマンドに基づいてドライバ７６によつてメカデツキ７４を駆動させる。これにより記録媒体上の所望の絶対アドレスまでサーチが行われ、ＡＴＦ(automatic tracking following)７７によつてトラツキングがとられて記録／再生処理部７３によつて記録媒体上に記録されたデータが再生される。ここで絶対アドレスは、伝送データに予め付加してもよく、またデイジタル信号受信装置４０内で付加してもよい。

【００４６】記録／再生処理部７３によつて再生された再生信号は、復調された後ローカルコンデイシヨナルアクセス４６でストレージ系の暗号が解除される。ストレージ系の暗号が解除された再生信号はエラー訂正され

て、フオーマツト変換部７２でフオーマツトが変換される。フオーマツト変換された再生信号はパケツト生成部７８でパケツト化され、デイジタルＩ／Ｆ６３、６２を介してパケツト分離部１６に送出されてパケツト分離される。パケツト分離された再生信号は、音声信号及び映像信号毎にそれぞれＭＰＥＧ音声デコーダ１７Ａ、ＭＰＥＧ映像デコーダ１７Ｂで圧縮が解凍される。

【００４７】圧縮が解凍された音声信号はデイジタルアナログ変換器（ＤＡＣ）７９でアナログ信号に変換されて出力される。圧縮が解凍された映像信号はＮＴＳＣ(national television system committee)エンコーダ８０でエンコードされる。またＣＰＵブロツク６４よりＮＴＳＣエンコーダ８１にユーザインタフエース等に関する一般データが入力され、当該エンコーダ８１でエンコードされた一般データはエンコーダ８０より出力される映像信号に付加されて出力される。

【００４８】以上の構成において、ソフトウエア情報PS_2をデイジタル信号受信装置４０に伝送する場合には、ソフトウエア供給部３１においてソフトウエア情報PS_2にソフトウエア系の暗号をかけた後、送出部３２において放送系の暗号をかけて２重のセキユリテイを確保した状態でデイジタル信号受信装置４０に伝送する。デイジタル信号受信装置４０では、ソフトウエア情報PS_2にかけられている放送系の暗号を解除した後デイジタルストレージ４１に記録する。デイジタルストレージ４１に記録されたソフトウエア情報PS_2を観る場合には、許可センタ４４で登録の確認をし、登録の確認がされると、ソフトウエア系の暗号が解除されてソフトウエア情報PS_2を観ることができる。

【００４９】以上の構成によれば、放送系のキーデータを全て共通にすると共に放送による課金データを無料とし、ソフトウエア情報PS_2を端末４０に供給する場合には、ソフトウエアデータPS_2に放送系及びソフトウエア系の暗号を２重にかけて伝送し、端末４０ではソフトウエアデータPS_2の放送系の暗号を解除してデイジタルストレージ４１にダウンロードする。これにより、ソフトウエア情報PS_2をデイジタルストレージ４１にダウンロードする際には、ソフトウエア情報PS_2にソフトウエア系の暗号がかけられているのでセキユリテイを確保することができる。

【００５０】また上述の構成によれば、パケツト分離部１６に送出される経路と記録再生部６１に送出される経路とを切り換えるスイツチング手段を設けたことにより、契約ユーザに対してはビデオオンデマンドとＶＴＲの長所をあわせもつたデイジタル信号伝送システムを提供することができる。

【００５１】また上述の構成によれば、ソフトウエア供給部３２でソフトウエア情報PS_2に変速再生処理を施してからデイジタル信号受信装置４０にソフトウエア情報PS_2を伝送したことにより、契約ユーザはストレージ４１に記録されたソフトウエア情報PS_2を変速再生することができる。

【００５２】また上述の構成によれば、伝送路の空き時間帯又は空き伝送路を利用して複数本の有料ソフトウエア情報PS_2を端末４０のストレージ４１にダウンロードすることができるので、ユーザはダウンロードした複数本のソフトウエア情報PS_2のうち、観たい時間に観たいものだけを観ることができる。すなわち観たいソフトウエア情報PS_2を選択する毎に課金処理が行われてストレージ４１内で再生制限が解除される。また衛星による伝送の場合のような１対１でないデイジタル信号伝送システムにおけるビデオオンデマンドを実現する手段として有効である。

【００５３】また上述の構成によれば、通常契約によるプログラムPS_1についての課金情報を管理する許可センタ２２へのアクセスとソフトウエア情報PS_2についての課金情報を管理する許可センタ４４へのアクセスとの切換えをモデム４３を介して制御したことにより、放送系とソフトウエア系の２つの独立した課金体系を構築することができる。

【００５４】（４）実施例によるデイジタル信号伝送システム

図１及び図２との対応部分に同一符号を付して示す図７において、９０は全体として実施例によるデイジタル信号伝送システムの概略構成を示している。デイジタル信号伝送システム９０では、所定のサービス例えば有料のソフトウエア情報PS_2を伝送する場合、ソフトウエア情報PS_2にストレージ系の暗号をかけた後、当該ソフトウエア情報PS_2にさらに放送系の暗号をかけて２重のセキユリテイを確保すると共に、ストレージ系の暗号をかける際に用いる暗号化キーＫｍをソフトウエア情報用のパーソナルキーＫｐ２を用いて暗号化している。

【００５５】ユーザがデイジタル信号伝送装置３０より伝送されるプログラムソースPS_1を観る場合、ユーザは放送局３０より郵送で送られてくるスマートカード１９を端末４０に差し込み、登録された放送系のＩＤ番号ＩＤ１を入力する。これにより、ＣＰＵ４２がモデム４３を介して許可センタ２２に登録の問い合わせをし、当該ユーザの登録が確認されると、放送局すなわちデイジタル信号伝送装置３０より放送系の暗号がかけられたプログラムソースＥｓ（Data）が送られてくる。

【００５６】すなわち放送局３０では、プログラムソースPS_1をデイジタル信号受信装置４０に伝送する場合、暗号化処理部５において暗号化キーＫｓによつてプログラムソースPS_1に放送系の暗号をかける。この暗号化キーＫｓはワークキー（Work Key、Ｋｗ）によつて暗号化され、またワークキーＫｗはユーザ毎に与えられる放送系のパーソナルキーＫｐ１によつて暗号化される。従つて暗号化処理部５は、放送系の暗号がかけられたプログラムソースＥｓ（Data）と、暗号化キーＥ（Ｋ

ｓ）及びワークキーＥ（Ｋｗ）とを多重化してデイジタル信号受信装置４０に伝送する。

【００５７】スマートカード１９には、暗号化キーＫｍを暗号化する際に用いられたパーソナルキーＫｐ１が含まれている。従つて端末４０では、暗号化されたワークキーＥ（Ｋｗ）の暗号がパーソナルキーＫｐ１によつて解除され、この暗号が解除されたワークキーＫｗによつて暗号化キーＥ（Ｋｓ）の暗号が解除される。さらにこの暗号が解除された暗号化キーＫｓによつて、プログラムソースＥｓ（Data）にかけられている放送系の暗号が解除される。暗号が解除されたプログラムソースPS_1はＭＰＥＧデコーダ１７で圧縮が解凍されてアナログ信号に変換された後、ＴＶに出力される。

【００５８】ユーザがソフトウエア情報PS_2をデイジタルストレージ４１にダウンロードしたい場合（この場合、上述のスイツチング手段はデイジタルストレージ４１に送出される経路に切り換わる）、ユーザはスマートカード１９を端末４０に差し込み、放送局３０に登録された放送系のＩＤ番号ＩＤ１を入力する。これにより、ＣＰＵ４２がモデム４３を介して許可センタ２２に登録の問い合わせをし、当該ユーザの登録が確認されると、放送局３０より放送系及びソフトウエア系の暗号がかけられたプログラムソースＥｓ｛Ｅｍ（Data）｝が送られてくる。

【００５９】すなわち放送局３０では、暗号化処理部３７においてソフトウエア情報用の暗号化キーＫｍによつてソフトウエア情報PS_2にストレージ系の暗号をかける。またこの暗号化キーＫｍはユーザ毎に与えられるソフトウエア情報用のパーソナルキーＫｐ２によつて暗号化される。暗号化されたソフトウエアデータＥｍ（Data）は暗号化処理部５に送出され、暗号化された暗号化キーＥ（Ｋｍ）は許可センタ４４に送られる。

【００６０】暗号化処理部５では、ソフトウエア系の暗号がかけられたソフトウエアデータＥｍ（Data）に暗号化キーＫｓを用いて放送系の暗号をかける。上述のように、この暗号化キーＫｓはワークキーＫｗによつて暗号化され、ワークキーＫｗはパーソナルキーＫｐ１によつて暗号化される。暗号化処理部５は、ソフトウエア系及び放送系の暗号が２重にかけられたソフトウエアデータＥｓ｛Ｅｍ（Data）｝と、暗号化キーＥ（Ｋｓ）及びワークキーＥ（Ｋｗ）とを多重化して端末４０に伝送する。

【００６１】端末４０では、当該端末４０にスマートカード１９が差し込まれているので、上述のように２重に暗号化されたソフトウエアデータＥｓ｛Ｅｍ（Data）｝の放送系の暗号が解除される。放送系の暗号が解除されたソフトウエアデータＥｍ（Data）はデイジタルストレージ４１に記録される。

【００６２】デイジタルストレージ４１に記録されたソフトウエアデータＥｍ（Data）を観る場合、ユーザはスマートカード９１を端末４０に差し込み、登録されたソフトウエア系のＩＤ番号ＩＤ２を入力する。これにより、ＣＰＵ４２がモデム４３を介して許可センタ４４に登録の問い合わせをする。当該ユーザの登録が確認されると、課金処理がなされた後、例えば電話回線を通じて許可センタ４４より暗号化キーＥ（Ｋｍ）がモデム４３を通じてスマートカード９１に入力され、暗号化キーＥ（Ｋｍ）の暗号が解除される。

【００６３】すなわちスマートカード９１には、ソフトウエア系の暗号化キーＫｍを暗号化する際に用いたパーソナルキーＫｐ２が含まれている。従つて暗号化キーＥ（Ｋｍ）の暗号がパーソナルキーＫｐ２によつて解除される。暗号が解除された暗号化キーＫｍはＣＰＵ４２を介して暗号解除部４６に送出される。

【００６４】暗号解除部４６では、暗号化キーＫｍによつてソフトウエアデータＥｍ（Data）にかけられているソフトウエア系の暗号を解除してＭＰＥＧデコーダ１７に送出する。ＭＰＥＧデコーダ１７では、暗号が解除されたソフトウエアデータPS_2の圧縮を解凍してアナログ信号に変換した後、ＴＶに出力する。

【００６５】以上の構成において、ソフトウエア情報PS_2をデイジタル信号受信装置４０に伝送する場合、ソフトウエア情報PS_2にソフトウエア系の暗号をかけた後放送系の暗号をかけて伝送すると共に、ソフトウエア系の暗号をかける際に用いた暗号化キーＫｍをパーソナルキーＫｐ２を用いて暗号化する。

【００６６】デイジタル信号受信装置４０では、スマートカード１９を用いてソフトウエアデータＥｓ｛Ｅｍ（Data）｝の放送系の暗号を解除した後デイジタルストレージ４１に記録する。デイジタルストレージ４１に記録されたソフトウエアデータＥｍ（Data）を観る場合、スマートカード９１によつて、暗号化キーＥ（Ｋｍ）の暗号が解除され、暗号が解除された暗号化キーＫｍによつてソフトウエアデータＥｍ（Data）にかけられているソフトウエア系の暗号が解除される。

【００６７】以上の構成によれば、ソフトウエア情報PS_2をデイジタル信号受信装置４０に伝送する際、ソフトウエア情報PS_2にソフトウエア系の暗号及び放送系の暗号をかけると共に、ソフトウエア系の暗号をかける際に用いた暗号化キーＫｍをパーソナルキーＫｐ２を用いて暗号化する。これにより、ソフトウエア情報PS_2のセキユリテイをさらに一段と確保することができる。

【００６８】また上述の構成によれば、暗号化された暗号化キーＥ（Ｋｍ）の暗号を解除するためのパーソナルキーＫｐ２をスマートカード９１に内蔵したことにより、ユーザは暗号化キーＥ（Ｋｍ）の暗号を簡易かつ確実に解除することができるので、観たい時間に観たいソフトウエア情報PS_2を観ることができる。

【００６９】（５）他の実施例

なお上述の実施例においては、契約ユーザが有料のソフ

トウエア情報を観る場合、契約ユーザは、ソフトウエア情報ＰＳ$_2$をストレージ４１にダウンロードしておき、ユーザが観たいときにデイジタルストレージ４１に記録されたソフトウエア情報ＰＳ$_2$を観る場合について述べたが、本発明はこれに限らず、図８に示すようにソフトウエア供給部３２及びデイジタル信号受信装置４０でパツケージ系システム１００を構築し、ソフトウエア供給部３２で暗号化したソフトウエア情報を記録媒体に記録してパツケージにし、このパツケージソフトウエア１０１を、例えば月極めなどで定期的にユーザに送つてもよい。

【００７０】この場合、図８に示すように、デイジタル信号受信装置４０だけで課金のシステムを構築することができる。またユーザは暗号化された複数のソフトウエア情報が記録されたソフトウエアパツケージ１０１をローコストで入手することによつて、観たい部分だけを課金処理して楽しむというような、ソフトウエア情報のパツケージ化による新しいソフトウエア情報の供給システムを構築することができる。ここでパツケージソフトウエア１０１には例えば10本分の映画が記録されている。

【００７１】また上述の実施例においては、放送系の許可センタ２２及びソフトウエア系の許可センタ４４を設けて、ＣＰＵ４２によつてモデム４３のシエアを制御することにより、２つのそれぞれ独立した課金体系を構築した場合について述べたが、本発明はこれに限らず、１つの許可センタで放送系及びソフトウエア系のプログラムに対する課金処理を行つてもよい。

【００７２】また上述の実施例においては、受信部６０に記録再生部６１が接続されたデイジタル信号受信装置４０を用いた場合について述べたが、本発明はこれに限らず、記録再生部６１を内蔵したデイジタル信号受信装置４０を用いてもよい。

【００７３】また上述の実施例においては、変速再生処理をソフトウエア供給部３２で行つた場合について述べたが、本発明はこれに限らず、端末すなわちデイジタル信号受信装置４０で変速再生処理を行つてもよい。

【００７４】また上述の実施例においては、通常契約によるプログラムソースＰＳ$_1$を観るためのスマートカード１９と、ソフトウエア情報ＰＳ$_2$を観るためのスマートカード９１を別個に設けた場合について述べたが、本発明はこれに限らず、１枚のスマートカードにスマートカード１９及びスマートカード９１の機能をもたせてもよい。

【００７５】また上述の実施例においては、ソフトウエア情報ＰＳ$_2$をデイジタルストレージ４１にダウンロードした場合について述べたが、本発明はこれに限らず、ソフトウエア情報ＰＳ$_2$をリアルタイムに観ることもできる。この場合、スイツチング手段をパケツト分離部１６に送出する経路に切り換えると共にスマートカード１９及び９１を端末４０に差し込む。これにより、ソフトウエア情報ＰＳ$_2$にかけられている放送系及びソフトウエア系の暗号が解除されてリアルタイムにソフトウエア情報ＰＳ$_2$を観ることができる。

【００７６】また上述の実施例においては、音声信号及び映像信号を帯域圧縮符号化してデイジタル信号受信装置４０に伝送した場合について述べたが、本発明はこれに限らず、映像信号だけを帯域圧縮符号化してデイジタル信号受信装置４０に伝送してもよい。

【００７７】

【発明の効果】上述のように本発明によれば、所定のサービスを提供する映像を伝送する場合、映像信号を帯域圧縮符号化したデイジタル信号に第１の暗号化処理をした後、当該デイジタル信号にさらに暗号化処理をして伝送することにより、映像信号に２重のセキユリテイを付加することができるので、一段とセキユリテイが確保されたデイジタル信号伝送方法を実現し得る。

【図面の簡単な説明】

【図１】本発明の実施例によるデイジタル信号伝送装置の構成を示すブロツク図である。

【図２】本発明の実施例によるデイジタル信号受信装置の構成を示すブロツク図である。

【図３】実施例によるデイジタル信号伝送装置の送出部の詳細構成を示すブロツク図である。

【図４】実施例によるデイジタル信号伝送装置のソフトウエア供給部の詳細構成を示すブロツク図である。

【図５】実施例によるデイジタル信号受信装置の受信部の詳細構成を示すブロツク図である。

【図６】実施例によるデイジタル信号受信装置の記録再生部の詳細構成を示すブロツク図である。

【図７】実施例によるデイジタル信号伝送システムの概略構成を示すブロツク図である。

【図８】パツケージ系のソフトウエア供給システムの説明に供するブロツク図である。

【図９】従来のデイジタル信号伝送装置の構成を示すブロツク図である。

【図１０】従来のデイジタル信号受信装置の構成を示すブロツク図である。

【図１１】従来のデイジタル信号受信装置においてソフトウエア情報をダウンロードする際の問題点の説明に供するブロツク図である。

【符号の説明】

１、３０……デイジタル信号伝送装置、２、２Ａ、２Ｂ、３３、３３Ａ、３３Ｂ……ＭＰＥＧエンコーダ、３、３Ａ、３Ｂ、３Ｃ、３Ｄ、３Ｅ、３４、３４Ａ、３４Ｂ、３４Ｃ、３４Ｄ、７８……パケツト生成部、４、３６……マルチプレクサ、５、３７……暗号化処理部、６、１２Ｃ……ＦＥＣ部、７……変調器、８……衛星、９……配信局、１０、４０……デイジタル信号受信装置、１１……アンテナ、１２……フロントエンド部、１２Ａ……チユーナ、１２Ｂ……復調器、１３……データ

17

取出し部、１４……デマルチプレクサ、１５……暗号解除部、１６、７１……パケット分離部、１７……ＭＰＥＧデコーダ、１７Ａ……ＭＰＥＧ音声デコーダ、１７Ｂ……ＭＰＥＧ映像デコーダ、１８、４１……デイジタルストレージ、１９、９１……スマートカード、２０、４２……ＣＰＵ、２１、４３……モデム、２２、４４……許可センタ、２３、４５……コンデイシヨナルアクセス、２４、４６……ローカルコンデイシヨナルアクセス、３１……送出部、３２……ソフトウエア供給部、３５……トリツクプレイ処理部、４７、５３……デイジタルＶＴＲ、４８、５７……データバス、４９、５４……パーソナルコンピユータ、５０、５１、５５、５６、５

18

８……データインタフエース、５２……アツプコンバータ、６０……受信部、６１……記録再生部、６２、６３……デイジタルインタフエース、６４……ＣＰＵブロツク、６５……ＥＥＰＲＯＭ、６６……モデムインタフエース、６７……ＶＲＡＭ、６８……ＧＰＵ、６９……ＲＯＭ、７０……ＤＲＡＭ、７２……フオーマツト変換部、７３……記録／再生処理部、７４……メカデツキ、７５……ＶＣＲコントローラ、７６……ドライバ、７７……ＡＴＦ、７９……ＤＡＣ、８０、８１……ＮＴＳＣエンコーダ、９０……デイジタル信号伝送システム、１００……パツケージ系システム、１０１……パツケージソフトウエア。

【図１】

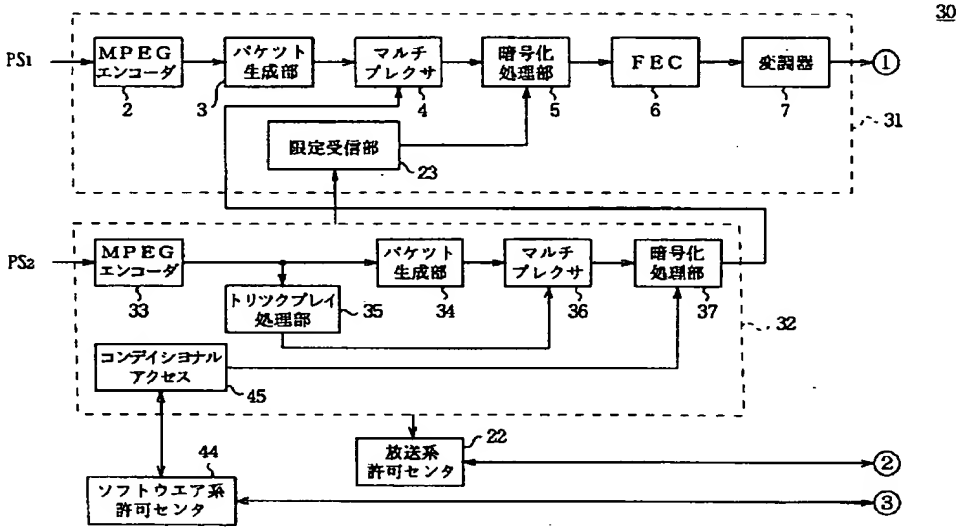


図１　デイジタル信号伝送装置の構成

【図９】

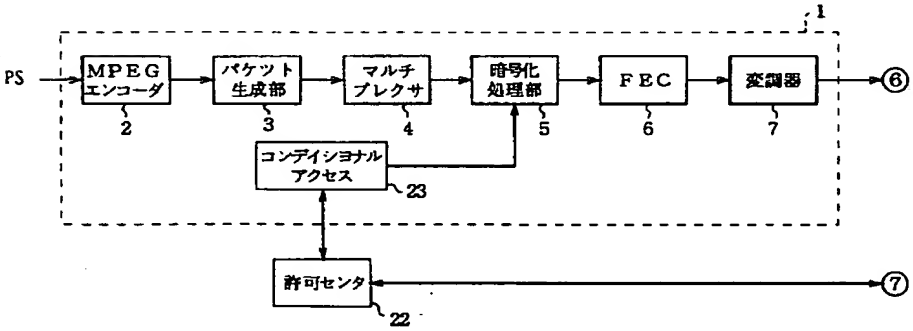


図９　従来のデイジタル信号伝送装置

【図２】

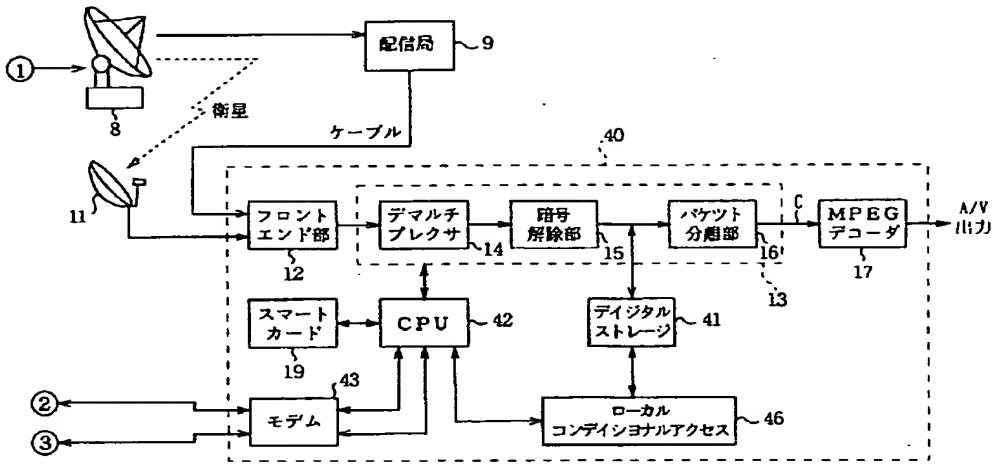


図２　デイジタル信号受信装置の構成

【図３】

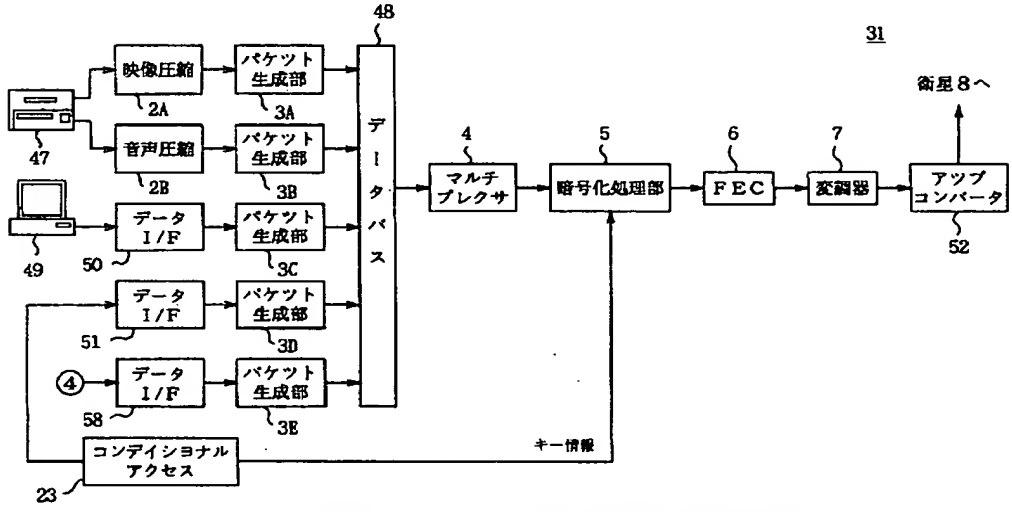


図３　実施例によるデイジタル信号伝送装置の送出部の構成

【図４】

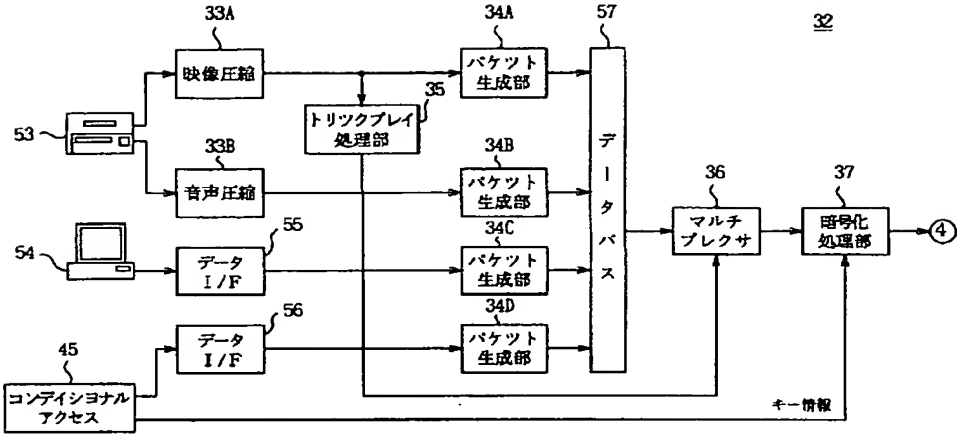


図４　実施例によるデイジタル信号伝送装置のソフトウエア供給部の構成

【図５】

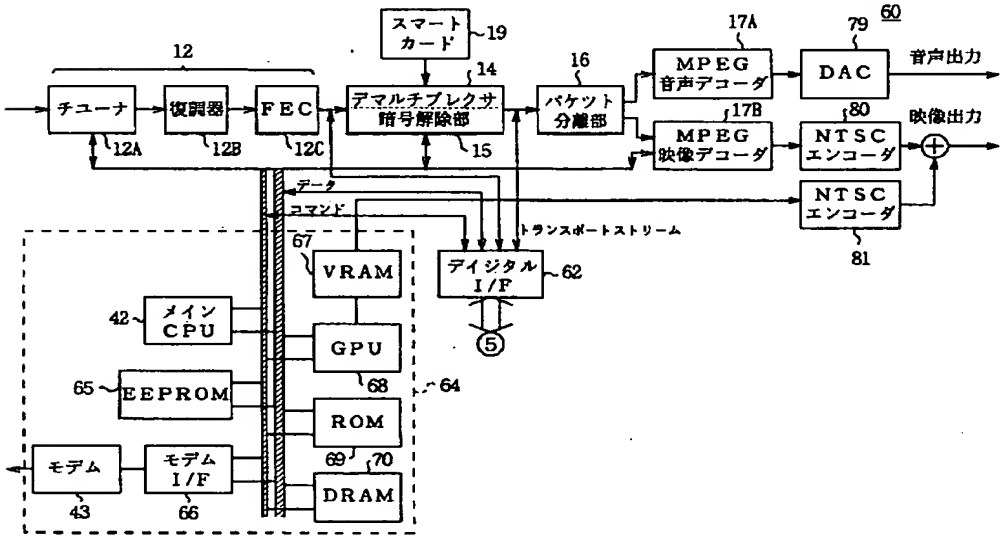


図５　実施例によるデイジタル信号受信装置の受信部の構成

【図６】

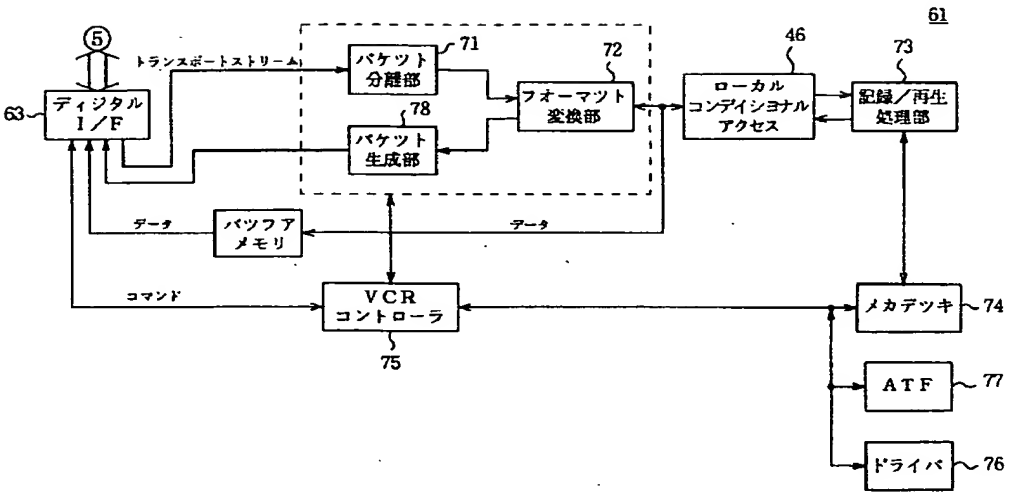


図６　実施例によるディジタル信号受信装置の記録再生部の構成

【図７】

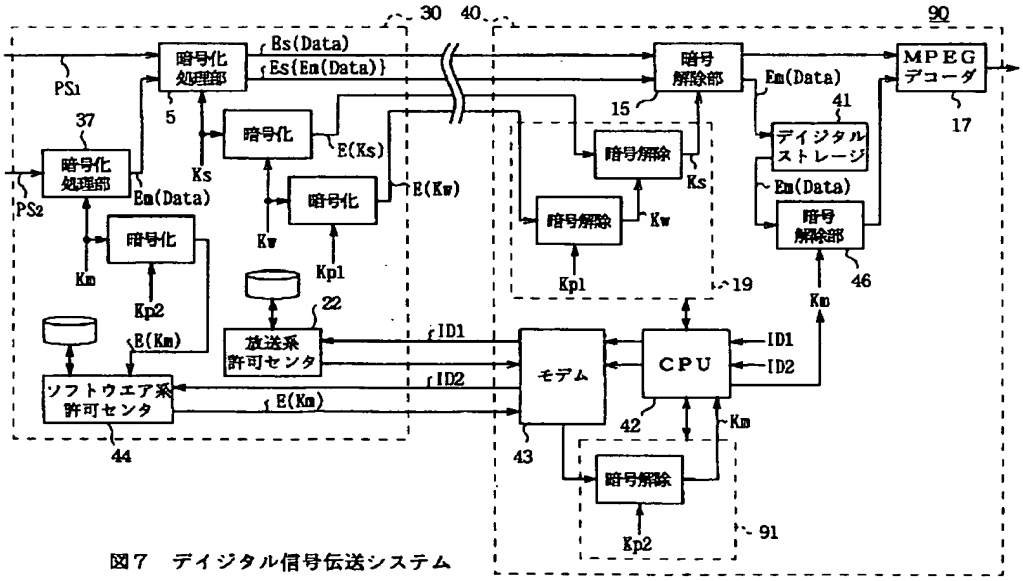


図７　ディジタル信号伝送システム

【図８】

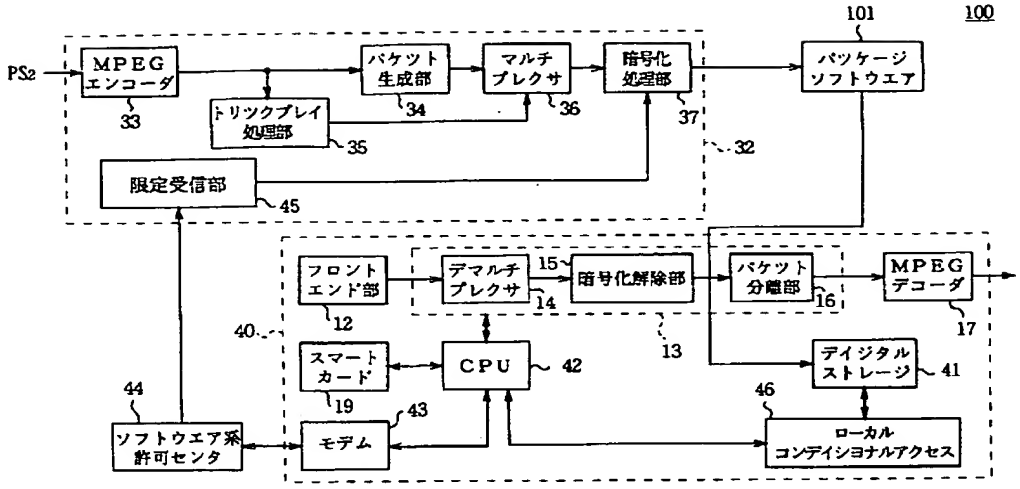


図８　パッケージ系のソフトウエア供給システム

【図１０】

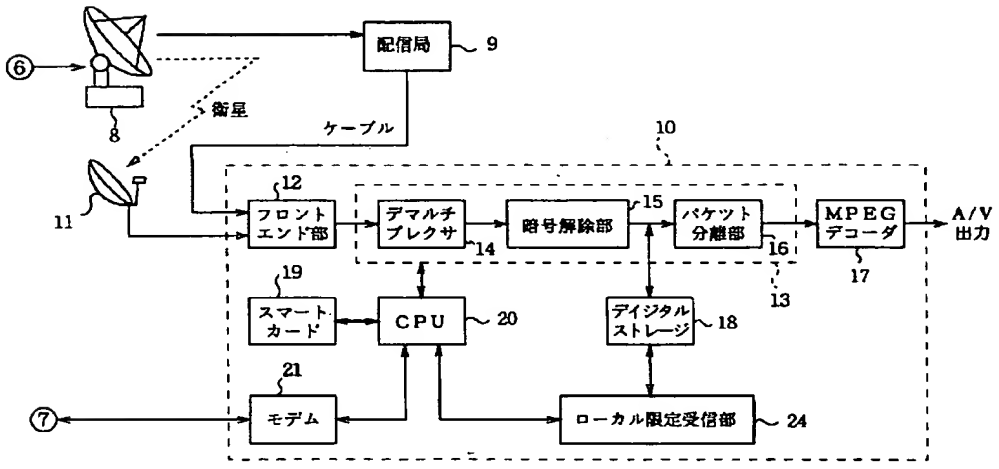


図１０　従来のデイジタル信号受信装置

【図１１】

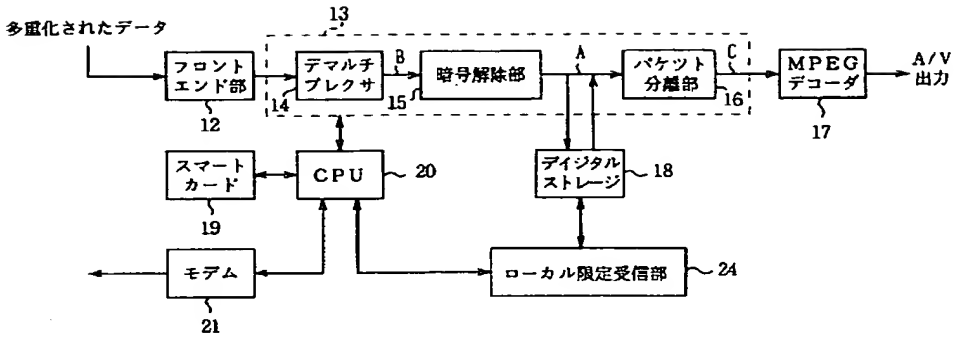


図１１　従来のデイジタル信号受信装置

フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｈ	1/00			F	
Ｈ０４Ｎ	7/167				